

Amendments to the Claims

This listing of claims will replace all prior version, and listings, of claims in the application.

Listing of Claims:

1. (currently amended) A method for providing security with a secure chip, the secure chip comprising a public/private key pair, the secure chip residing within a computer, comprising the steps of:

- (a) creating a migratable keyblob using a first random number, wherein the migratable keyblob contains a key;
- (b) wrapping the migratable keyblob with a public key of the key's parent key;
- (c) encrypting the first random number with a pass phrase for a user of the key;
- (d) storing the encrypted first random number; and
- (e) migrating the migratable keyblob from the computer to itself the security chip residing within the computer.

2. (original) The method of claim 1, wherein the creating step (a) comprises:

- (a1) generating a first random number by the secure chip;
- (a2) scrambling the key; and
- (a3) creating the migratable keyblob by XOR the first random number with the scrambled key.

3. (original) The method of claim 1, wherein the encrypting step (c) comprises:

- (c1) receiving the pass phrase for the user of the key;

(c2) generating a second random number by hashing the pass phrase;

(c3) generating a third random number by applying a mass generation function (MGF)

to the second random number;

(c4) converting the third random number into a string with a same length as the first random number; and

(c5) generating a fourth random number by XOR the first random number with the third random number.

4. (original) The method of claim 3, wherein the storing step (d) comprises:

(d1) storing the fourth random number

5. (original) The method of claim 4, further comprising:

(f) receiving the pass phrase;

(g) obtaining the third random number from the pass phrase by reversing the MGF and hash used to generate it;

(h) obtaining the first random number by XOR the third random number with the stored fourth random number;

(i) sending the first random number and the migratable keyblob to the secure chip;

(j) unwrapping the migratable keyblob by the secure chip using the secure chip's private key;

(k) obtaining a scrambled key by XOR the migratable keyblob with the first random number; and

(l) unscrambling the key.

6. (original) The method of claim 5, further comprising:

(m) returning a normal blob for the unscrambled key; and

(n) discarding the normal blob.

7. (original) A method for providing security with a secure chip, the secure chip comprising a public/private key pair, the secure chip residing on a computer, comprising the steps of:

(a) generating a first random number by the secure chip;

(b) creating a migratable keyblob using the first random number, wherein the migratable keyblob contains a key;

(c) wrapping the migratable keyblob with the public key of the secure chip;

(d) receiving a pass phrase for a user of the key;

(e) generating a second random number based on the pass phrase;

(f) generating a third random number based on the second random number;

(g) generating a fourth random number based on the first random number and the third random number;

(h) storing the fourth random number; and

(i) migrating the migratable keyblob from the computer to itself the security chip residing on the computer.

8. (original) The method of claim 7, wherein the creating step (b) comprises:

(b1) scrambling the key; and

(b2) creating the migratable keyblob by XOR the first random number with the scrambled key.

9. (original) The method of claim 7, wherein the generating step (e) comprises:

(e1) generating the second random number by hashing the pass phrase.

10. (original) The method of claim 7, wherein the generating step (f) comprises:

(f1) generating the third random number by applying a MGF to the second random number; and

(f2) converting the third random number into a string with a same length as the first random number.

11. (original) The method of claim 7, wherein the generating step (g) comprises:

(g1) generating the fourth random number by XOR the first random number with the third random number.

12. (original) The method of claim 7, further comprising:

(j) receiving the pass phrase;

(k) obtaining the third random number from the pass phrase;

(l) obtaining the first random number from the third random number and the stored fourth random number;

- (m) sending the first random number and the migratable keyblob to the secure chip;
- (n) unwrapping the migratable keyblob by the secure chip using the secure chip's private key;
- (o) obtaining a scrambled key by XOR the migratable keyblob with the first random number; and
- (p) unscrambling the key.

13. (original) The method of claim 12, wherein the obtaining step (k) comprises:
(k1) obtaining the third random number from the pass phrase by reversing a MGF and Hash used to generate it.

14. (original) The method of claim 12, wherein the obtaining step (l) comprises:
(l1) obtaining the first random number by XOR the third random number with the stored fourth random number.

15. (original) The method of claim 12, further comprising:
(q) returning a normal blob for the unscrambled key; and
(r) discarding the normal blob.

16. (original) A computer readable medium with program instructions for providing security with a secure chip, the secure chip comprising a public/private key pair, the secure chip residing on a computer, comprising the instructions for:

- (a) creating a migratable keyblob using a first random number, wherein the migratable keyblob contains a key;

- (b) wrapping the migratable keyblob with a public key of the key's parent key;
- (c) encrypting the first random number with a pass phrase for a user of the key;
- (d) storing the encrypted first random number; and
- (e) migrating the migratable keyblob from the computer to itself the security chip
residing on the computer.

17. (original) The medium of claim 16, wherein the creating instruction (a) comprises instructions for:

- (a1) generating a first random number by the secure chip;
- (a2) scrambling the key; and
- (a3) creating the migratable keyblob by XOR the first random number with the scrambled key.

18. (original) The medium of claim 16, wherein the encrypting instruction (c) comprises instructions for:

- (c1) receiving the pass phrase for the user of the key;
- (c2) generating a second random number by hashing the pass phrase;
- (c3) generating a third random number by applying a mass generation function (MGF) to the second random number;
- (c4) converting the third random number into a string with a same length as the first random number; and
- (c5) generating a fourth random number by XOR the first random number with the third random number.

19. (original) The medium of claim 18, wherein the storing instruction (d) comprises instructions for:

(d1) storing the fourth random number

20. (original) The medium of claim 19, further comprising instructions for:

(f) receiving the pass phrase;

(g) obtaining the third random number from the pass phrase by reversing the MGF and hash used to generate it;

(h) obtaining the first random number by XOR the third random number with the stored fourth random number;

(i) sending the first random number and the migratable keyblob to the secure chip;

(j) unwrapping the migratable keyblob by the secure chip using the secure chip's private key;

(k) obtaining a scrambled key by XOR the migratable keyblob with the first random number; and

(l) unscrambling the key.

21. (original) The medium of claim 20, further comprising instructions for:

(m) returning a normal blob for the unscrambled key; and

(n) discarding the normal blob.

22. (currently amended) A computer readable medium with program instructions for

providing security with a secure chip, the secure chip comprising a public/private key pair, the secure chip residing on a computer, comprising the instructions for:

- (a) generating a first random number by the secure chip;
- (b) creating a migratable keyblob using the first random number, wherein the migratable keyblob contains a key;
- (c) wrapping the migratable keyblob with the public key of the secure chip;
- (d) receiving a pass phrase for a user of the key;
- (e) generating a second random number based on the pass phrase;
- (f) generating a third random number based on the second random number;
- (g) generating a fourth random number based on the first random number and the third random number;
- (h) storing the fourth random number; and
- (i) migrating the migratable keyblob from the computer to itself the security chip on the computer.

23. (original) The medium of claim 22, wherein the creating instruction (b) comprises instructions for:

- (b1) scrambling the key; and
- (b2) creating the migratable keyblob by XOR the first random number with the scrambled key.

24. (original) The medium of claim 22, wherein the generating instructions (e) comprises instructions for:

(e1) generating the second random number by hashing the pass phrase.

25. (original) The medium of claim 22, wherein the generating instructions (f) comprises instructions for:

(f1) generating the third random number by applying a MGF to the second random number; and

(f2) converting the third random number into a string with a same length as the first random number.

26. (original) The medium of claim 22, wherein the generating instruction (g) comprises instructions for:

(g1) generating the fourth random number by XOR the first random number with the third random number.

27. (original) The medium of claim 22, further comprising instructions for:

(j) receiving the pass phrase;

(k) obtaining the third random number from the pass phrase;

(l) obtaining the first random number from the third random number and the stored fourth random number;

(m) sending the first random number and the migratable keyblob to the secure chip;

(n) unwrapping the migratable keyblob by the secure chip using the secure chip's private key;

(o) obtaining a scrambled key by XOR the migratable keyblob with the first random number; and

number; and

- (p) unscrambling the key.

28. (original) The medium of claim 27, wherein the obtaining instruction (k) comprises instructions for:

(k1) obtaining the third random number from the pass phrase by reversing a MGF and Hash used to generate it.

29. (original) The medium of claim 27, wherein the obtaining instruction (l) comprises instructions for:

(l1) obtaining the first random number by XOR the third random number with the stored fourth random number.

30. (original) The medium of claim 27, further comprising:

- (q) returning a normal blob for the unscrambled key; and
- (r) discarding the normal blob.